High Capacity Robust Medical Image Data Hiding using CDCS with Integrity Checking

Sunita V. Dhavale[1], and Suresh N. Mali[2]
[1] Department of Information Technology, Marathwada Mitra Mandal's College of Engineering, Pune, Maharashtra-411052, India.
Email: sunitadhavale75@rediffmail.com
[2] Department of Computer Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra-411037, India.
Email: snmali@rediffmail.com

***Abstract*—While transferring electronic patient report (EPR) data along with corresponding medical images over network, confidentiality must be assured. This can be achieved by embedding EPR data in corresponding medical image itself. However, as the size of EPR increases, security and robustness of the embedded information becomes major issue to monitor. Also checking the integrity of this embedded data must be needed in order to assure that retrieved EPR data is original and not manipulated by different types of attacks. This paper proposes high capacity, robust secured blind data hiding technique in Discrete Cosine Transform (DCT) domain along with integrity checking. A new coding technique called Class Dependent Coding Scheme (CDCS) is used to increase the embedding capacity. High imperceptibility is achieved by adaptively selecting the efficient DCT blocks. Even a slight modification of stego image in embedded region as well as in ROI (Region of Interest) can be detected at receiver so to confirm that attack has been done. The embedding scheme also takes care of ROI which is diagnostically important part of the medical images and generates security key automatically. Experimental results show that the proposed scheme exhibits high imperceptibility as well as low perceptual variations in Stego-images. Security and robustness have been tested against various image manipulation attacks.**

***Index Terms*—Medical image, EPR, Data hiding, Stego image, ROI, Robustness, Security, Integrity Check.**

I. Introduction

Telemedicine application requires transferring Electronic Patient Report (EPR) data and corresponding medical images over network for further diagnostic purpose. While sharing medical images and EPR in telemedicine et al. [1], we need to protect of both medical images and EPR data as well as to save as much space as possible in order to reduce the cost of storage and increase the speed of transmission. Both these goals can be achieved by effective embedding of EPR in corresponding medical image itself.

Aim of proposed EPR data hiding is to increase data hiding capacity without perceptual degradation of the medical image along with integrity checking et al. [2, 7]. A new CDCS coding scheme has been proposed in this paper that will not only reduces the number of bits to represent EPR data but also increases the perceptual quality of the image for the given data hiding capacity. Before embedding this encoded EPR data in medical image et al. [3], high imperceptibility as well as robustness is achieved by adaptively selecting the area of an image in which to hide data using energy thresholding method et al. [2].

Further, one must also guarantee that the region in which we have embedded sensitive and confidential EPR data is not tampered by any malicious manipulations et al. [4]. Thus there is a need for integrity checking that must assure both EPR data and image has not been modified by unauthorized person. So secure hash can be calculated over this sensitive region and these hash bits can be embedded in diagnostically less important region et al. [4] like border (black surrounding) or very low frequency region outside ROI of medical image using fragile spatial domain techniques like simple LSB substitution method. So even simple cutting or cropping the image at border region can loose these embedded hash bits and attack can be confirmed. The stego key that is automatically generated based on embedding factors like randomization, redundancy, interleaving, energy thresholding and JPEG quality factor provides multiple levels of security.

II. Proposed System

The proposed embedding scheme consists of text processing phase and image processing phase as shown in Fig. 1 Text processing phase makes the stream of EPR encoded bits ready for embedding, whereas, image processing phase embeds these bits into the corresponding medical image. At the time of execution of these phases the embedding parameters (r, n, w1, w2, seed, QF, x1, y1, x2, y2) are provided as an input that gets reflected in automatically generated embedding key.

A. CDCS

Proposed system assigns fixed codes in CDCS to each character by considering their probability of frequency of occurrences as shown in Fig. 2 The EPR characters are then categorized in three different nonoverlapping special classes as Class-A (most frequently appearing character set), Class-B (Average frequently appearing) and Class-C (Less frequently appearing characters). Further, the number of bits needed to represent each character in the respective classes is achieved by assuming only capital letters,

Corresponding Author: Mrs. Sunita V. Dhavale, M.E.(CSE-IT), MMCOE, Pune-411052, India.

DOI: 01.IJSIP.02.01.175

alphanumeric and few special characters. Based on Huffman encoding, the variable length class code (CC) have been designed to represent each class as given in Table 1.

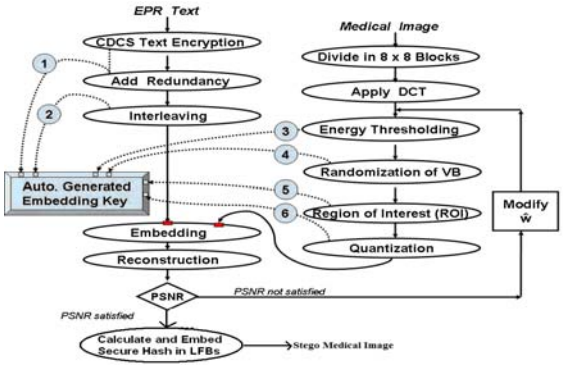

Figure 1. Proposed System: Multilevel security

Any character in each Class will be represented by only 4 bits prefixed by CC (1-bit or 2-bit). Therefore, CC along with 4 bit character code can distinguish 48 different characters as shown in Table 1, which are sufficient to represent any EPR. Huffman coding is complex and also assigns codes with more than 32 bits for non repeating characters whereas ASCII gives fixed length codes for the characters. The proposed CDCS combines the advantages of both fixed length and variable length coding to get less number of bits to represent same information compared to fixed 7-bit ASCII codes.

If N1, N2 and N3 are the total number of characters belonging to Class-A, Class-B and Class-C respectively, Total number of bits to be embedded is given by,

$$m = (N_1 + 2N_2 + 2N_3) + 4h \quad (1)$$

Where, $h = N_1 + N_2 + N_3$, i.e. total number of characters in EPR file.

Percentage Bit Saving (PBS) is given by,

$$PBS = \left[1 - \left(\frac{m}{7h}\right)\right] \times 100\ \% \quad (2)$$

B. Redundancy and Interleaving

Robustness against various attacks can be achieved by adding redundancy for each bit prior to embedding et al. [7, 8]. Interleaving of bits will disperse subsequent bits from each other throughout the image. Hence, even if any block of Stego-image undergoes with attack, EPR bits can be successfully recovered from other blocks. CDCS encryption along with specified number of redundancy bits added (r) and number of interleaving bits (n) provides two security levels 1 and 2 as shown in Fig. 1.

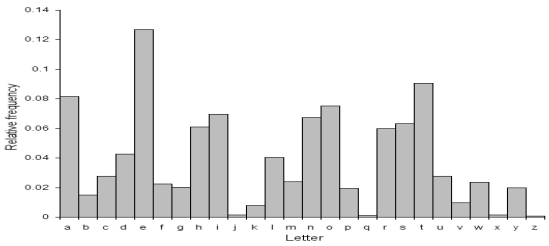

Figure 2. Probability of occurrences for EPR characters

Table 1: CDCS: Class CODE with Fixed Code within Each Class

Class A CC=1 (1bit)	Class B CC=00 (2bits)	Class C CC=01 (2bits)	4-Bit Code
Blank	M	0	0000
.	U	1	0001
E	G	2	0010
T	Y	3	0011
A	P	4	0100
O	W	5	0101
N	B	6	0110
R	V	7	0111
I	K	8	1000
S	X	9	1001
H	J	(	1010
D	Q	)	1011
L	Z	=	1100
F	,	*	1101
C	-	%	1110
:	_	+	1111

C. Energy Thresholding

A sequence of lower and middle frequency non-zero quantized DCT coefficients of randomly generated valid blocks are used to embed final processed bits. After dividing the image into 8 x 8 non overlapping blocks two dimensional DCT is computed for each block along with its energy. The blocks having energy greater than the threshold energy will only be considered for embedding. Energy threshold (Et) is calculated as,

$$E_t = \hat{w} \cdot MVE \quad (3)$$

where, ŵ = Energy threshold factor and MVE = Mean Value of Energy given by,

DOI: 01.IJSIP.02.01.175

$$MVE = \frac{1}{z}\sum_{k=1}^{z} E_k \quad (4)$$

where, z = Number of 8 x 8 non-overlapping blocks of the image and E_k= Energy of kth block which is given by,

$$E_k = \sum_{i=1}^{7}\sum_{j=1}^{7} \| C_{ij} \|^2 \quad (5)$$

where C_{ij} = Two dimensional DCT coefficients.
Classify the DCT blocks by define two different energy thresholds w_1 and w_2 using (3), in such a way that, $w_1 >> w_2$.

As blocks having more energy can embed information bits with minimal distortion et al. [7], all blocks having energy more than E_{t1} (decided by w_1) will only be considered for embedding and treated as Valid Blocks (VBs) while blocks having energy lesser than E_{t2} (decided by w_2) are selected as very Low Frequency DCT Blocks (LFBs) where a small size hash bits can be embedded safely without causing more distortion to medical image.

D. Adaptive Energy Threshold Factor ($\hat{w}$)

There is always a trade-off between ŵ and number of VBs. As the value of ŵ increases, we get less number of VBs. In this scheme, one can adaptively modify the value of ŵ by monitoring the PSNR of reconstructed image with respect to given value of PSNR as shown in Fig. 1. This embedding parameter ŵ gives security level 3.

E. Randomization, ROI and Quantization

Security level 4 is achieved by randomly selecting the VBs. The random number generator based on a seed is used to select random VBs. Diagnostically important area of medical image can be defined by specifying the diagonal indices (X1, Y1) and (X2, Y2). The VBs coming in the vicinity of ROI will not be considered for embedding. These specified indices give security level 5. The randomly selected VBs are then quantized for the given value of QF. After the process of quantization the non-zero predefined DCT coefficients are considered for embedding the data. The embedding parameter QF gives security level 6.

F. Embedding and Reconstruction

The embedding is carried out by suitably modifying the DCT coefficients of the valid blocks finally selected after the process of quantization. If the bit is logically 'zero', the coefficient is rounded to 'even' number, otherwise to 'odd' number. Finally stego-image is reconstructed by applying inverse DCT and combining all 8 x 8 image blocks. Take secure hash of Embedded VB's as well as ROI blocks and encrypt and embed these hash bits into LSB's of randomly selected pixels of LFBs. This hash embedding stage used for integrity checking of both embedded data and ROI gives security level 7.

Fig. 1 shows all the steps of the proposed embedding scheme. The experimentation shows that after embedding the EPR bits of information, the Stego-images gives PSNR value more than 40dB.

G. EPR Data Retrieval

Fig. 3 gives automatically generated embedding key (AGEK) during the process of embedding along with the respective security levels. This embedding key has to be shared with the receiver through a secret channel. The embedding key has 52 bits (n=4, r=4, seed= 16, ŵ (both w1 and w2) = 8, QF = 8, x1-y1= 6 and x2-y2 =6). It is difficult to break the key for particular combination decided by the embedding algorithm. The extraction algorithm consists of all the image processing steps that are carried out at the time of embedding final processed bits. Recalculate secure hash of those embedded VB's as well as ROI blocks. Extract encrypted hash bits from LSB's of randomly selected pixels of LFBs and decrypt it.

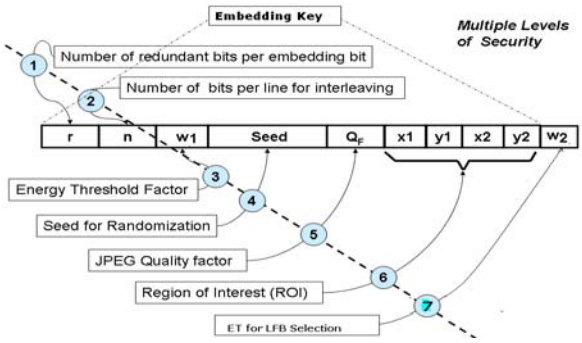

Figure 3. Bit format of AGEK

Compare both hash bits if equal, then image is authenticated and we can retrieve embedded EPR data safely and EPR information can be reconstructed using CDCS.

III. Experimental Results

We used grayscale 512 x 512 L-Spine (Lumbar Spine) medical images as shown in following Fig. 4a for our experiments. Experimentation is performed to check tamper detection capability of the system under various attacks (intentional and unintentional). Fig. 4b shows corresponding stego image, when 4 bits of EPR are embedded per 8 x 8 DCT block. The locations chosen for each VB block are (2,2), (3,0), (0,3) and (0,2). The 320 bit encrypted hash code is embedded in LSBs of 8 pixels per LFB block. The quality factor QF=50 chosen.

For a given E_{t1} (decided by w1) and E_{t2} (decided by w2) in Table 2, Fig. 5a shows corresponding VB Blocks or region of images where EPR data is embedded while Fig. 5b shows corresponding LFB Blocks or region of images where Hash data is embedded. Here w2 is selected in such a way that all LFBs fall generally in border black region. The PSNR observed for the stego images is above 40db. Any attack like small pixel stains made in VB region or EPR embedded region, which could not be visible by normal eye is detected at receiver side successfully.

DOI: 01.IJSIP.02.01.175

A. Effect of CDCS

Table 3 shows comparison of CDCS and ASCII codes for various number of EPR characters. It can be observed that increase in data hiding capacity is the result of PBS with proposed CDCS.

Table 2. Et1 and Et2 choices

Medical Image	EPR Bits	w1	w2	PSNR(dB)	PSNR(dB) after attack
L-Spine	2534	3705	10	44.65	40.43
Shoulder	2098	1977	10	47.14	46.61

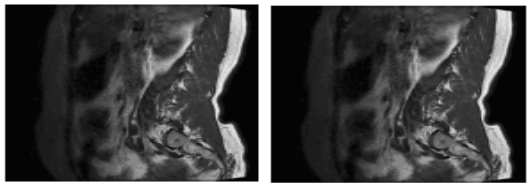

Figure 4. Original and Stego L-Spine Medical Image

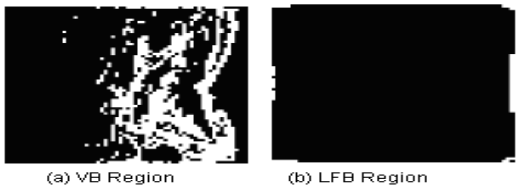

Figure 5. VB and LFB Region

Table 3: Capacity Performance of CDCS over ASCII

EPR characters	ASCII bits	CDCS bits	PBS (%)
506	3542	2814	20.55
584	4088	3244	20.65

B. Perceptual Transparency

Fig. 4a and Fig. 4b shows original and Stego 512 x 512 'L-Spine' images respectively. The locations chosen per block are at (2,2), (3,0), (0,3) and (0,2) to embed 270 EPR characters. The 'QF =70' and the EPR data has been embedded with 'w1 =0.5'. The PSNR observed for the Stego-image is 47.5982. Proposed scheme shows PSNR greater than 38 dB for embedding up to 3000 EPR bits in 'L-spine' images.

C. Robustness Test

The proposed system is robust and gives very less Bit Error Rate (BER) against JPEG compression attack, image tampering attack, image manipulation attack and change in contrast value.

CONCLUSIONS

In this paper, we proposed a method for the secure transmission of medical images by using both DCT and LSB substitution along with new CDCS encoding scheme for EPR data in order to increase hiding capacity. First we embedded EPR data into the medical images and then we embedded hash bits to guarantee the integrity of the medical images transmitted. Proposed CDCS can be used as effective coding scheme for EPR data hiding in medical images which increases the embedding capacity and provides better perceptual quality of Stego-image. Effective use of redundancy and interleaving enhances the robustness of the scheme against various attacks like JPEG compression, image tampering and image manipulation. Seven layered security achieved due to redundancy, interleaving, energy thresholding, random-ization, ROI quantization and Hash embedding stage makes the proposed system most secured.

Also further the stego key generated can be further encrypted using any public key encryption algorithm and can be transmitted in secure way to the receiver along with stego image. Also even slight modification to embedded region and ROI part can be detected unambiguously at receiver side. Thus the proposed system can effectively be used for high volume of EPR data hiding in medical images with reasonable robustness and security.

REFERENCES

[1] Gonzalo Alvarez1, Shujun Li and Luis Hernandez, "Analysis of security problems in a medical image encryption system," *Computers in Biology and Medicine*, vol. 37 (2007) 424–427.

[2] M. Fallahpour and M. H. Sedaaghi, "High capacity lossless data hiding based on histogram modification", *IEICE Electron. Express*, Vol. 4, No. 7 (2007) 205–210

[3] J. Zain and Malcolm Clarke, "Security in Telemedicine: Issues in Watermarking Medical Images", 3rd International Conference : Science of Electronic, Technologies of Information and Telecommunications (2005)

[4] B. Planitz, A. Maeder, "Medical Image Watermarking: A Study on Image Degradation", *Proc. Australian Pattern Recognition Society Workshop on Digital Image Computing*, WDIC 2005, Brisbane, Australia (2005)

[5] G. S. Pavlopoulos, D.Koutsouris, "Multiple Image Watermarking Applied to Health Information Management", *IEEE Transactions on Information Technology in Biomedicine*, vol. 10.4 (2006) 722 – 732

[6] K. A. Navas, S. A. Thampy, and M. Sasikumar, "EPR Hiding in medical images for telemedicine," *International Journal of Biomedical Sciences* Volume 3.1 (2008) 44– 47

[7] K. Solanki, N. Jacobsen, U. Madhow, B.S.Manjunath and S. Chandrashekhar, "Robust Image-Adaptive Data hiding using Erasure and Error Correction," *IEEE Transactions on image processing*, Volume 13, (2004) 1627–1639.

[8] S. N. Mali and R. M. Jalnekar., "Imperceptible and Robust Data Hiding using Steganography Against Image Manipulation," *International Journal of Emerging Technologies and Applications in Engineering, Technology and Sciences*, (IJ-ETA-ETS) (2008) 84–91.

[9] G. J. Simmons, "The prisoners' problem and subliminal channel", in *Advances in Cryptology. Proceedings of Crypto 83* (D. Chaum, ed.), Plenum Press (1984) 51–67.

[10] Neil F. Johnson and S. Jajodia, "Exploring Steganography. Seeing Unseen", *IEEE Computer*, vol. 31.2 (1998) 26 – 34.

[11] Min. Wu , "Joint Security and Robustness Enhancement for Quantization Embedding", *IEEE Transactions* 0-7803-7750-8/03(2003)483–486.

DOI: 01.IJSIP.02.01.175